# National Infrastructure Protection Center
# CyberNotes

*Issue #2000-16* *August 14, 2000*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between July 28 and August 10, 2000. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

| **Vendor/ Operating System** | **Software Name** | **Vulnerability/ Impact** | **Patches/Workarounds/Alerts** | **Common Name** | **Risk*** | **Attacks/Scripts** |
|---|---|---|---|---|---|---|
| Alt-N[1]<br>Windows 95/98/NT 4.0/2000 | MDaemon 2.8 | A vulnerability exists in WorldClient, which could be used by a malicious user to read the e-mail of a remote user. | Upgrade to 2.8.7.5 which is available at:<br>**Windows NT:**<br>ftp://ftp.altn.com/MDaemon/Archive/2.8/md2875patchNT.exe<br>**Windows 9x:**<br>ftp://ftp.altn.com/MDaemon/Archive/2.8/md2875patch9X.exe<br>You will need MDaemon version 2.8.5.0 to install this fix. | MDaemon Session ID Hijacking | Medium | Bug discussed in newsgroups and websites. |

[1] NTBugtraq, August 9, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Bajie[2] | Java HTTP Server 1.0 | A vulnerability exists in the Java servlet that ships with the Bajie Web server, which might reveal critical physical path information. In addition, by sending the server a URL that contains four dots, a malicious user can make the server access any file on the system by specifying its relative path from the root directory. | Workaround for the critical path information vulnerability: Remove/disable the offending servlet, /servlet/test/pathInfo/test<br>No workaround or patch available for the local system compromise vulnerability at time of publishing. | Bajie Webserver Multiple Vulnerabilities | Medium | Bug discussed in newsgroups and websites.<br>Exploit has been published. |
| BEA Systems[3]<br>Windows 98/NT 4.0/2000, Unix | WebLogic Enterprise 5.1; WebLogic Express 5.1x; WebLogic Server 5.1x | Two "show code" vulnerabilities exist which could allow a malicious user to view the source code of any file within the web document root of the web server or access and view unauthorized files in the root directory. | Please refer to security advisory, BEA00-03.00, which can be found at: http://developer.bea.com/alerts/index.html | WebLogic FileServlet Show Code | Medium | Bug discussed in newsgroups and websites.<br>Exploit has been published. |
| BEA Systems[4]<br>Windows NT 4.0 | WebLogic Enterprise 5.1; WebLogic Express 5.1x; WebLogic Server 5.1x | A vulnerability exists which could let a malicious user compile and execute any arbitrary file within the web document root directory of the server as if it were a JSP/JHTML file, even if the file type is not .JSP or JHTML. | Please refer to security advisory, BEA00-04.00, which can be found at: http://developer.bea.com/alerts/index.html | WebLogic SSIServlet Show Code | **High** | Bug discussed in newsgroups and websites.<br>Exploit has been published. |
| CheckPoint Software[5] | Firewall-1 3.0, 4.0, 4.1 | A vulnerability exists when certain unauthorized connections are sent from an external RSH/REXEC server to an internal (protected) RSH/REXEC client. This can only be done if the FireWall-1 administrator specifically enabled RSH/REXEC in the Properties window. | Check Point Software hotfix Service Packs available at: http://www.checkpoint.com/techsupport/index.html | Firewall-1 Unauthorized RSH/REXEC Connection | Low/ **High**<br>**(High if best DDoS practices not in place)** | Bug discussed in newsgroups and websites. |

[2] MDMA Crew, July 30, 2000.
[3] Foundstone, Inc. Security Advisory, FS-072800-9-BEA, July 28, 2000.
[4] Foundstone, Inc. Security Advisory, FS-073100-10-BEA, July 31, 2000.
[5] Securiteam, August 7, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Cisco Systems[6] | Cisco IOS Software releases for the GSR starting with release 11.2(15)GS1A | A vulnerability exists in IOS Software running on all models of Gigabit Switch Routers (GSRs) configured with Gigabit Ethernet or Fast Ethernet cards, which may cause packets to be forwarded without correctly evaluating configured access control lists (ACLs). In addition to circumventing the access control lists, it is possible to stop an interface from forwarding any packets. | Cisco is offering free software upgrades to remedy this vulnerability which are available at:<br>http://www.cisco.com/ | Cisco Gigabit Switch Router with Fast/Gigabit Ethernet Cards ACL Bypass/ Denial of Service | Medium/ **High**<br>**(High if best DDoS practices not in place)** | Bug discussed in newsgroups and websites.<br>Vulnerability has appeared in the Press and other public media. |
| Computer Associates[7]<br>Unix | ARCServeIT 6.63 Linux | A vulnerability exists in /usr/CYEagent/agent.cfg, which could allow a malicious user to gain root privileges or execute arbitrary code. | No workaround or patch available at time of publishing. | ARCserveIT ClientAgent Temporary File | **High** | Bug discussed in newsgroups and websites. |
| Concurrent Version Systems[8] | CVS 1.10.8 | Two security vulnerabilities exist: any binary in the server using CVS/Checkin.prog or CVS/Update.prog can be executed; and the server can be instructed to create any file at any location in client machine. | No workaround or patch available at time of publishing. | CVS Multiple Vulnerabilities | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Deerfield.com[9] | FTP Serv-U 2.5e | A Denial of Service vulnerability exists when a string containing a large number of null bytes is sent. | Upgrade to version 2.5f available at:<br>http://www.deerfield.com/products/index.cfm?loc=ftp | FTP Serv-U Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| GNU[10]<br>Unix | Userv 1.0.0 | A vulnerability exists in the fd swapping algorithm, which could let local malicious users carry out unauthorized actions or take control of service user accounts. | Upgrade to version 1.0.1 available at:<br>ftp://ftp.chiark.greenend.org.uk/users/ian/userv/userv-1.0.1.tar.gz | Userv Service Program Environment Corruption | Medium | Bug discussed in newsgroups and websites. |
| Hewlett-Packard[11]<br>Unix | HP-UX 11.0 | A buffer overflow vulnerability exists in the seated utility /usr/bin/bd. which could cause the program to exit with a memory fault. | No workaround or patch available at time of publishing. | HP-UX Buffer Overflow | Low | Bug discussed in newsgroups and websites. |

[6] Cisco Security Advisory, CI-00.06, August 2, 2000.
[7] Bugtraq, July 28, 2000.
[8] Bugtraq, July 29, 2000.
[9] Blue Panda Vulnerability Announcement, August 4, 2000.
[10] Debian Security Advisory, Debian-00-015, July 28, 2000.
[11] Bugtraq, July 27, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Kirk Bauer[12]<br>Unix | DiskCheck 3.1.1<br>DiskCheck is included with RedHat "Rawhide" and "Pinstripe". | A symlink vulnerability exists which could give local malicious users elevated privileges. This could allow the creation of files with root permissions. | This fixed in current versions of RedHat "Rawhide" and "Pinstripe". | DiskCheck Race Condition | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| LIDS[13]<br>Unix | LIDS 0.9.7 | If LIDS is disabled using the 'security=0' option at boot time, all users logging in to the system will be able to behave as root. | Upgrade to LIDS 0.9.8 available at: http://www.lids.org/lids-0.9.8-2.2.16.tar.gz | LIDS Root Level Access When Disabled | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Microsoft[14]<br>Windows 95/98/NT 4.0/2000 | Access 2000, Word 2000, | MS Word and MS Access 2000 allow executing arbitrary programs if a Word document is opened. This may be exploited also by visiting a web page with IE or opening/previewing HTML e-mail message with Outlook. | No workaround or patch available at time of publishing. | Microsoft Office 2000 Mail Merge | **High** | Bug discussed in newsgroups and websites. Exploits have been published.<br>Vulnerability has appeared in the Press and other public media. |
| Microsoft[15]<br>Windows 95/98/NT 4.0/2000 | Excel 2000, PowerPoint 2000, Word 2000 | A security vulnerability exists which could allow a malicious user to construct a HyperText Markup Language (HTML) file that, when read, would crash a Microsoft Office 2000 application or potentially run arbitrary or malicious code. | Frequently asked questions regarding this vulnerability and the patch can be found at http://www.microsoft.com/technet/security/bulletin/fq00-056.asp | Microsoft Office HTML Object Tag | **High** | Bug discussed in newsgroups and websites.<br>Vulnerability has appeared in the Press and other public media. |
| Microsoft[16]<br>Windows 95/98/NT 4.0/2000 | Internet Explorer 4.x, 5.x | Two security vulnerabilities exists, which could allow a malicious web site operator to read (but not add, change, or delete) files on the computer of a visiting user. The two vulnerabilities are: the "Scriptlet Rendering" vulnerability; and a new variant of the "Frame Domain Verification" vulnerability. | Frequently asked questions regarding this vulnerability and the patch can be found at http://www.microsoft.com/technet/security/bulletin/fq00-055.asp<br>Customers who apply this patch will also be protected against the vulnerabilities discussed in the Security Bulletins MS00-033, MS00-039, and MS00-049.<br>In addition, for IE 5.5 systems only, this patch also eliminates the vulnerability discussed in MS00-042. | Internet Explorer Scriptlet Rendering | Medium | Bug discussed in newsgroups and websites. |

[12] Bugtraq, August, 5, 2000.

[13] Bugtraq, August 3, 2000.

[14] Georgi Guninski Security Advisory #17, August 7, 2000.

[15] Microsoft Security Bulletin, MS00-056, August 10, 2000.

[16] Microsoft Security Bulletin, MS00-055, August 9, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Microsoft[17]<br>Windows NT 4.0/2000 | Internet Information Server (IIS) 4.0, 5.0 | A security vulnerability exists, under very restricted conditions, which could allow a malicious user to gain additional permissions to certain types of files hosted on a web server. | Frequently asked questions regarding this vulnerability and the patch can be found at http://www.microsoft.com/technet/security/bulletin/fq00-057.asp | Windows NT File Permission Canonicalization | Medium | Bug discussed in newsgroups and websites. |
| Microsoft[18]<br>Windows NT 4.0/2000 | NT 4.0 Workstation, Server, Server Enterprise Edition, Terminal Server Edition, Windows 2000 Professional, Server, Advanced Server | A security vulnerability exists, which could allow a malicious user to cause code of his/her choice to run when another user subsequently logged onto the same machine. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-052.asp | Windows NT Relative Shell Path | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| **Microsoft**[19]<br>**Windows 95/98/NT 4.0/2000**<br>***Microsoft releases a patch.***[20]<br>***Microsoft re-releases the patch.***[21] | **PowerPoint 2000; Internet Explorer 5.01** | **A vulnerability exists which could allow the execution of programs when viewing a web page or HTML e-mail, which in turn could provide full control of a targeted computer.**<br>***Microsoft has released a patch that eliminates this vulnerability.***<br>***The security bulletin was re-released to announce the availability of a patch for the vulnerability in Internet Explorer.*** | **Unofficial Workaround (Georgi Guninski):**<br>**Disable Active Scripting or Disable Run ActiveX controls and plug-ins.**<br>***Microsoft Excel 2000 and PowerPoint 2000:***<br>http://officeupdate.microsoft.com/2000/downloaddetails/Addinsec.htm<br>***Microsoft PowerPoint 97:***<br>http://officeupdate.microsoft.com/downloaddetails/PPt97sec.htm<br>*IE Script vulnerability:*<br>***http://www.microsoft.com/windows/ie/download/critical/patch11.htm*** | ***Office HTML Script and IE Script Vulnerabilities*** | **High** | **Bug discussed in newsgroups and websites. Exploit has been published.** |

[17] Microsoft Security Bulletin, MS00-057, August 10, 2000.
[18] Microsoft Security Bulletin, MS00-052, July 28, 2000.
[19] Georgi Guninski Security Advisory #13, June 27, 2000.
[20] Microsoft Security Bulletin, MS00-049, July 14, 2000.
[21] Microsoft Security Bulletin, MS00-049, re-released August 9, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Microsoft[22]<br>Windows 95/98 | Windows 95, 98, 98 Second Edition | A security vulnerability exists, which could be used to cause an affected system to fail, and depending on the number of affected machines on a network, potentially could be used to flood the network with superfluous data. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-054.asp | Windows Malformed IPX Ping Packet | Low | Bug discussed in newsgroups and websites. |
| Microsoft[23]<br>Windows NT 2000 | Windows NT 2000 | A security vulnerability exists, which could allow a malicious user logged onto a Windows 2000 machine to become an administrator on the machine or gain privileged access. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-053.asp | Microsoft Windows 2000 Service Control Manager Named Pipe Impersonation | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| **Multiple Vendors[24]**<br>**Unix**<br>***New exploit released.[25]*** | **Conectiva Linux 4.0-4.2, 5.0; Debian Linux 2.2, 2.3; RedHat Linux 6.0-6.3; Trustix Secure Linux 1.0, 1.1** | **A vulnerability exists in the rpc.statd daemon, which could let remote malicious users gain root access to the system or could cause the rpc.statd program to execute arbitrary code.** ***A new advanced exploit code for RedHat Linux 6.x string formatting vulnerability in StatD has been released.*** | **Contact your vendor for update** | **Multiple Vendor Rpc.statd Remote Format String Stack Overwrite** | **High** | **Bug discussed in newsgroups and websites. Exploit script has been published.** |
| Multiple Vendors[26, 27]<br>Unix | GNU Mailman 2.0beta3, 2.0beta4 | The wrapper program supplied with the mailman package has a format vulnerability, which could be exploited to obtain the privileges of the mailman user. This user has read and write access to all files of the mailman package. | Upgrade to version 2.0beta5 located at: http://www.gnu.org/software/mailman/mailman.html | GNU Mailman Local Format String Stack Overwrite | Medium | Bug discussed in newsgroups and websites. |
| Multiple Vendors[28, 29]<br>Unix | Luca Deri ntop 1.2a7-9 | If ntop is run with the Web interface, it allows any user to connect and access all files on the host machine, including files, which are only readable by root. | **RedHat:**<br>ftp://updates.redhat.com/powertools/6.2/<br>**Debian:**<br>http://security.debian.org/dists | Linux Ntop Unauthorized File Retrieval | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[22] Microsoft Security Bulletin, MS00-054, August 3, 2000.
[23] Microsoft Security Bulletin, MS00-053, August 2, 2000.
[24] Security Alert Consensus #054, July 20, 2000.
[25] Securiteam, August 8, 2000.
[26] Conectiva Linux Security Announcement, 2000-08-02, August 2, 2000.
[27] Red Hat, Inc. Security Advisory, RHSA-2000:030-03, August 3, 2000.
[28] Red Hat, Inc. Security Advisory, RHSA-2000:049-02, August 8, 2000.
[29] Debian Security Advisory, August 7, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Multiple Vendors[30, 31]<br>Unix | NetBSD 1.4.1 & 1.4.2 x86, arm32, SPARC, Alpha; OpenBSD 2.4-2.7; RedHat Powertools 6.0-6.2 | A buffer overflow exists in the mopd (Maintenance Operations Protocol loader daemon), which could allow a remote malicious user to execute arbitrary code on the affected machine. | **NetBSD:**<br>http://cvsweb.netbsd.org/bsdweb.cgi/basesrc/usr.sbin/mopd/mopd/process.c<br>**OpenBSD:**<br>ftp://ftp.openbsd.org/pub/OpenBSD/patches/2.7/common/018_mopd.patch<br>**RedHat Powertools**<br>ftp://updates.redhat.com/powertools/ | Multiple Vendor Mopd Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Multiple Vendors[32, 33, 34]<br>Unix | Larry Wall Perl 5.004_05, 5.005_003, 5.6 | An interactions between some security checks performed by SuidPerl, and the /bin/mail program creates a vulnerability that allows local malicious users to execute commands with root privileges. | Patch available at:<br>http://www.securityfocus.com/data/vulnerabilities/patches/suidperl1.patch<br>**TurboLinux:**<br>ftp://ftp.turbolinux.com/pub/updates<br>**SuSE:**<br>ftp://ftp.suse.com/pub/suse<br>**RedHat:**<br>ftp://updates.redhat.com | SuidPerl Mail Shell Escape | **High** | Bug discussed in newsgroups and websites. Exploit scripts have been published. |
| Netscape[35]<br>Windows 95/98/NT 4.0/2000, Unix | Communicator 4.05-4.08, 4.0, 4.5-4.51, 4.6-4.61, 4.72-4.74 | A pair of new capabilities in Java, one residing in the Java core and the other in Netscape's Java distribution, allows creating of a remote management tool that can be used to compromise a remote system. The first allows Java to open a local server that can be accessed by arbitrary clients. The second allows Java to access arbitrary URLs, including local files. | **Workaround:**<br>Until a fix becomes available, Java should be disabled in the browser. | Netscape URL File Read and Listening Socket Vulnerabilities | Medium/ **High** | Bug discussed in newsgroups and websites. Exploit script has been published.<br>Vulnerability has appeared in the Press and other public media. |
| Network Associates[36]<br>Windows NT 4.0 | Net Tools PKI Server 1.0, 1.0Hotfix1, 1.0Hotfix2 | Three vulnerabilities exist: one involves the 'strong.exe' program (a buffer overflow); another involves a directory traversal security hole (also known as the 'dotdotdot' vulnerability); and the last one involves a formatting strings parsing problem. | Hotfix 3 available at:<br>http://www.nai.com/asp_set/download/upgrade/find.asp | Net Tools Multiple Vulnerabilities | Low | Bug discussed in newsgroups and websites. Exploits have been published. |

[30] Bugtraq, August 8, 2000.
[31] Red Hat, Inc. Security Advisory, RHSA-2000:050-01, August 8, 2000.
[32] TurboLinux Security Announcement, TLSA2000018-1, August 9, 2000.
[33] SuSE Security Announcement, August 10, 2000.
[34] Red Hat, Inc. Security Advisory, RHSA-2000:048-02, August 8, 2000.
[35] Securiteam, August 7, 2000.
[36] CORE SDI Security Advisory, August 2, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Novell[37]<br>Windows 95/98 | Novell Client 3.1, Symantec Norton AntiVirus 5.0 | With the Novell Netware Client installed, Norton Antivirus and its auto-protect service is disabled after the first user to log in logs out. This leaves the system vulnerable to attacks, which the auto-protect software may have prevented. | No workaround or patch available at time of publishing. | Norton Antivirus with Novell Client Autoprotection Disabling | **High** | Bug discussed in newsgroups and websites. |
| PCCS-Linux[38]<br>Unix | MySQL Database Admin Tool 1.2.3, 1.2.4 | A vulnerability exists in the file structure, which can be used to expose the MySQL administrator password. | Upgrade to versions 1.2.5 and later which are available at: http://pccs-linux.com/public/list.php3?bn=agora_pccslinux | MySQL Database Admin Tool Username/ Password Exposure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| RedHat[39]<br>Unix | University of Massachusetts scheme 3.2-11 | The package umb-scheme contains files that have been given inappropriately world-writable permissions, which could be exploited by a malicious user to root privileges. | University of Massachusetts scheme 3.2-11 available at: ftp://updates.redhat.com/6.2/sparc/umb-scheme-3.2-12.sparc.rpm | Linux Umb-scheme World Writable | **High** | Bug discussed in newsgroups and websites. |
| Silicon Graphics Inc.[40]<br>Unix | IRIX 6.2 | A buffer overflow vulnerability exists in the libgl.so library in the way the HOME environment variable is handled which could let a malicious user locally gain root privileges. | No workaround or patch available at time of publishing. | IRIX libgl.so Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Silicon Graphics Inc.[41]<br>Unix | IRIX 6.2, 6.3 | A buffer overflow vulnerability exists in the command line parsing code portion of the lpstat program, which could lead to a local root compromise. | No workaround or patch available at time of publishing. | IRIX Lpstat Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Silicon Graphics Inc.[42]<br>Unix | IRIX 6.2, 6.3 | A buffer overflow vulnerability exists in the command line parsing code portion of the dmplay program, which could lead to a local root compromise. | No workaround or patch available at time of publishing. | IRIX Dmplay Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |

[37] Bugtraq, July 28, 2000.
[38] Securiteam, August 10, 2000.
[39] Red Hat, Inc. Security Advisory, RHSA-2000:047-03, August 7, 2000.
[40] Bugtraq, August 2, 2000.
[41] Bugtraq, August 2, 2000.
[42] Bugtraq, August 2, 2000.

| **Vendor/ Operating System** | **Software Name** | **Vulnerability/ Impact** | **Patches/Workarounds/Alerts** | **Common Name** | **Risk*** | **Attacks/Scripts** |
|---|---|---|---|---|---|---|
| Silicon Graphics Inc.[43]<br>Unix | IRIX 6.2, 6.3 | A buffer overflow vulnerability exists in the command line parsing code portion of the gr_ogview program, which could lead to a local root compromise. | No workaround or patch available at time of publishing. | IRIX Gr_osview Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Silicon Graphics Inc.[44]<br>Unix | IRIX 6.2-6.4 | The truncate() system call on a number of versions of the IRIX operating system (with the xfs file system) does not properly check permissions before truncating a file, which could let unprivileged users access files to which they would otherwise not have write access. | No workaround or patch available at time of publishing. | IRIX Xfs Truncate() Privilege Check | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Silicon Graphics Inc.[45]<br>Unix | IRIX 6.5, 6.5.1, 6.5.2m, 6.5.3, 6.5.3f , 6.5.3m, 6.5.4, 6.5.6-6.5.8 | A race condition vulnerability exists in the inpview program, which could lead to a local root compromise. | No workaround or patch available at time of publishing. | IRIX Inpview Race Condition | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Sun Microsystems, Inc. [46]<br>Unix | AnswerBook2 1.3x, 1.4-1.4.2 | Two security vulnerability exist which could allow a malicious user to access the administration of the AB2, as well as running arbitrary commands on the remote host. | Patch available at: http://www.sun.com/software/ab2/dwnld_versions.html | AnswerBook2 Remote Command Execution and Administration Interface Access Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| SuSE[47]<br>Unix | SuSE 6.1-6.4<br>knfsd, all versions | Due to incorrect string parsing in the code, a remote malicious user could gain root privileges on the machine running the vulnerable rpc.kstatd. | Update available at: ftp://ftp.suse.com/pub/suse | SuSE String Parsing | **High** | Bug discussed in newsgroups and websites. |
| Symantec[48]<br>Windows NT | Norton Antivirus 5.02 | A local user on a Windows NT/2000 machine can use Norton Antivirus' scheduler service to gain elevated privileges. | **Workaround (Securiteam):** Since the vulnerability occurs due to a normal user being able to write to the Norton installation directory, this can be solved by setting the AntiVirus directory permissions to read only and execute. | Norton Antivirus Elevated Privileges | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[43] Bugtraq, August 2, 2000.
[44] Bugtraq, August 3, 2000.
[45] Bugtraq, August 2, 2000.
[46] Sun Microsystems, Inc. Security Bulletin, #00196, August 7, 2000.
[47] SuSE Security Announcement, August 10, 2000.
[48] Securiteam, August 10, 2000.

| Vendor/ Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Tech-Source[49]<br>Unix | Raptor GFX PGX32 2.3.1 | Multiple vulnerabilities exists in the pgxconfig application, which could let a local malicious user run arbitrary commands as root. | No workaround or patch available at time of publishing.<br>**Unofficial Workaround (Bugtraq):**<br>Remove the '+s' bit from pgxconfig. | Raptor GFX Config Tool Vulnerabilities | **High** | Bug discussed in newsgroups and websites.<br>Exploit script has been published. |
| Tumbleweed[50]<br>Windows 95/98/NT 4.0/2000 | Messaging Management System (MMS) 4.3, 4.5, 4.6 | A default user account 'sa' is created which uses no password. This could let a remote malicious user connect to the database and delete or modify data. | Patch available at:<br>http://thompson.tumbleweed.com/NewKB/bulletin/UPFiles/saPassword.exe | Tumbleweed MMS No Default Password | Medium | Bug discussed in newsgroups and websites. |

*Risk is defined in the following manner:

**High -** A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

**Medium -** A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

**Low -** A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 29 and August 10, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 40 scripts, programs, and net-news messages containing holes or exploits were identified.

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| August 10, 2000 | Fscan112.zip | A fast command line port scanner for Windows, which will scan both TCP and UDP, ports, grabs banners, has adjustable time-outs, and scans ranges of IPs. |
| August 10, 2000 | Nsat-1.22.tgz | A fast bulk security scanner designed to audit remote network services and check for versions, security problems, gather information about the servers and the machine and much more. |

[49] Bugtraq, August 2, 2000.
[50] Bugtraq, August 10, 2000.

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| August 9, 2000 | Return-rst-1.0.tar.gz | A firewalling tool for Linux 2.2.xx systems using IPCHAINS. It uses the netlink device to capture packets and sends TCP RST packets in response to TCP connection requests. Normal IPCHAINS only allows you to drop packets, or reject packets with an ICMP error message. With Return-RST, you can make it look like there is no server listening, rather than giving away that they're being filtered to the attacker. |
| August 9, 2000 | Suidperlhack.pl | Perl exploit script for the SuidPerl v5.00503 and below local root vulnerability. |
| August 9, 2000 | Vetescan-8-9-2000.tar.gz | A bulk vulnerability scanner containing programs to scan Windows NT and UNIX systems for the latest Trojans/remote exploits, a scanner for the vulnerabilities of single hosts (with or without host checking), a tool for scanning multiple hosts, a scanner for class A/B/C networks, and fixes for various vulnerabilities. |
| August 9, 2000 | Vsl-8-9-2000.tgz | A shell script which checks local Unix security, including checking for rootkits, log permissions, home/root directory accessibility, inetd services, /etc/security, SUID/SGID files, World writable files, Unowned files, rhosts, and cracks passwd/shadow. |
| August 9, 2000 | Wakeonlan-0.40.tar.gz | This Perl script sends 'magic packets' to wake-on-lan enabled Ethernet adapters, in order to remotely power up a PC. |
| **August 9, 2000** | **Word-access.txt** | **Demonstration exploit for the Microsoft Word MS Word and MS Access 2000 (with or without Service Release 1a) vulnerability.** |
| **August 8, 2000** | **BOHTTPD.vulnerability.txt** | **Exploit text for the Netscape URL File Read and Listening Socket Vulnerabilities.** |
| **August 8, 2000** | **BOHTTPD-0.1.tar.gz** | **Exploit script for the Netscape URL File Read and Listening Socket Vulnerabilities.** |
| August 8, 2000 | Statdx.c | Exploit script for the Rpc.statd Remote Format String Stack Overwrite vulnerability. |
| August 8, 2000 | Xitdos.c | Denial of Service script, which exploits the Xitami Webserver v2.4d3, and below are vulnerability. |
| August 8, 2000 | Xperl.pl | Local root exploit script for the SuidPerl v5.00503 and below vulnerability. |
| August 7, 2000 | Saint-2.1.2.tar.gz | A security assessment tool based on SATAN. |
| August 5, 2000 | Core-sdi.net.tools | Perl proof of concept exploits for the NAI Net Tools PKI Server vulnerabilities. |
| August 5, 2000 | TFAK4.zip | TFAK v4.0 is a client for 22 remote access Trojans, and removes 366 remote access Trojans and 9 file joiners. This is the first and only Trojan scanner, which is able to find new, unknown Trojans. |
| August 5, 2000 | Whisker-1.4.0.tar.gz | A very stealthy CGI scanner, which is scriptable and is tailored to do flexible web scanning including over 200 checks. |
| August 5, 2000 | Xperl.sh | Local root exploit script for the SuidPerl v5.00503 and below vulnerability. |
| August 4, 2000 | Tin_bof.c | A local linux/x86 buffer overflow exploit which spawns a gid=news shell if /usr/bin/tin is setgid. |
| August 3, 2000 | Ethereal-0.8.11.tar.gz | A GTK+-based network protocol analyzer, that lets you capture and interactively browse the contents of network frames. |
| **August 3, 2000** | **Irx_truncate.c** | **Exploit script for the IRIX Xfs Truncate() Privilege Check vulnerability.** |
| August 3, 2000 | Nessus-1.0.4.tar.gz | A remote security scanner for Linux, BSD, Solaris and other systems which is multithreaded, plugin-based, has a GTK interface, and currently performs over 340 remote security checks. |
| August 3, 2000 | Servu25e.txt | Perl proof of exploit script for the FTP Serv-U 2.vulnerability. |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| **August 2, 2000** | **012.txt** | **Local root exploit script for the Raptor Pgxconfig vulnerability.** |
| **August 2, 2000** | **Dmplay.c** | **Exploit script for the IRIX gr_osview Buffer Overflow vulnerability.** |
| **August 2, 2000** | **Gr.c** | **Exploit script for the IRIX gr_osview Buffer Overflow vulnerability.** |
| **August 2, 2000** | **In-race.c** | **Exploit script for the IRIX Inpview Race Condition vulnerability.** |
| **August 2, 2000** | **Libgl.c** | **Exploit script for the IRIX libgl.so Buffer Overflow vulnerability.** |
| **August 2, 2000** | **Lpstat.c** | **Exploit script for the IRIX lpstat Buffer Overflow vulnerability.** |
| August 2, 2000 | Nscan0666b14f.zip | A fast port scanner for Windows (up to 200 ports per second) for both hosts and large networks with numerous features. |
| **August 2, 2000** | **Raptor.sh** | **Exploit script for the Raptor GFX Config Tool vulnerability.** |
| August 2, 2000 | Rpc.statd.x86.c | Linux/x86 rpc.statd remote root exploit. |
| August 1, 2000 | Nmap-2.54BETA2.tgz | A utility for port scanning large networks. |
| August 1, 2000 | Trinux-070.tgz | Trinux transparently converts ordinary x86 PCs into a powerful network security workstations by combining Linux Slackware 7.1 with all of the most powerful precompiled Open Source security/monitoring tools. |
| July 31, 2000 | Ncsa1-3.c | NCSA Httpd v1.3 remote root exploit. |
| July 31, 2000 | Sara-3.1.6.tar.gz | A security analysis tool based on the SATAN model. |
| July 31, 2000 | Sourcescan.pl | Sourcescan.pl looks through C source code for common vulnerabilities, including strcpy, gets, strcat, sprintf, fscanf, scanf, vsprintf, realpath, getopt, getpass, streadd, strecpy, strtrns, getenv, and setenv. |
| July 30, 2000 | FS-072800-9-BEA.txt | Proof of concept exploit for BEA's WebLogic show code vulnerabilities. |
| July 30, 2000 | Fuzz-0.5.1.tar.gz | Fuzz searches for new security vulnerabilities by generating random strings, which can be passed in several ways to programs to see if they can be made to crash or hang. |
| July 29, 2000 | Stjude_LKM-0.02.tar.gz | Saint Jude LKM is a Linux Kernel Module for the 2.2.0 series of kernels, which implements the Saint Jude model for improper privilege transitions. This will permit the discovery of local, and ultimately, remote root exploits during the exploit itself. |

## *Script Analysis*

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

*No scripts were submitted during the two-week period covered by this issue of CyberNotes.*

## *Trends*

**DDoS/DoS:**

- **A new backdoor exploit program called "Brown Orifice," takes advantage of vulnerability in Netscape and Java. For more information, please see NIPC System Assessment 00-0521, which is available at** http://www.nipc.gov/warnings/assessments/2000/assess00-052.htm**.**
- **Numerous sites, that still run an old version of Apache, have been struck by a Windows-based DDoS attacks originating from over 500 different IP address.**
- The "Trinoo" DDoS program has attacked over 250 Korean Networks.
- A simple exploit/DoS tool named "octo" or "octopus" has the ability to shut down services remotely. This little program opens as many sockets with a remote host as can be supported by both.
- A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attack.

**Probes/Scans:**

- An increase in linuxconf scanning.
- An increase in scanning for the Bind vulnerability.
- An increase in distributed scans from Israel.
- An increase in scans on port 21 (when WuFTPD 2.5.0 was shown vulnerable).
- A continuation of scans to port 109 (pop2 exploit).
- A continuation of probes to UDP Port 137 (NetBIOS Name Service).
- Increasing reports of scans to known Trojan ports. System administrators should consult their intrusion detection system and firewall logs for unusual port scans.

**Other:**

- Another variant of the "ILOVEYOU" computer virus was detected in Ireland.
- Chat clients and Internet Relay Chat (IRC) networks pose a serious security risk due to recent viruses like the I Love You and Life-Stages bugs. Both were programmed to take advantage of instant messaging software and chat rooms to spread themselves rapidly across computers and flaws in chat client software and could be easily exploited by malicious users to plant and launch malicious code in corporate networks. Users could be also tricked into communicating sensitive information or downloading files containing malicious code via chat clients.
- An increase in sites being probed or root compromised related to input validation vulnerabilities in many FTP databases.
- A recent malicious programs exploiting the default behavior of Windows operating systems to hide file extensions from the user. This behavior can be used to trick users into executing malicious code by making a file appear to be something it is not. Multiple e-mail-borne viruses are known to exploit this vulnerability.
- A steady number of reports of intruders exploiting unprotected Windows networking shares.
- Reports indicate domain name registration information continues to be maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.

## *Viruses*

**Polyboot.512 (Boot Virus):** This virus carries encrypted viral code and is capable of infecting the MBR (Master Boot Record) of hard disks, as well as the boot sectors of floppies. In addition, it incorporates stealth techniques to prevent it from being detected. When the virus is run, it goes memory resident, and can be detected from DOS due to the fact that it takes up 2KB of conventional memory. This virus does not infect files or carry out destructive actions.

**VBS_Kakworm.B (Aliases: Kakworm.B, VBS_Dayworm, Wscript.KakWorm.B) (Windows Worm):** This direct action worm is compatible with the Windows Scripting Host interpreter, which means that a user must have MS IE 5 or a browser that supports Windows Scripting for this worm to execute. Once executed, this worm modifies the default signature in Outlook Express and embeds itself in e-mail it sends out to all lists in the infected user's address book. The worm is compatible with both English and French versions of Windows. This worm uses the same security hole as VBS_BubbleBoy. By simply viewing the e-mail with the embedded worm in the preview pane, the user becomes infected. If the current system date is 11 and the hour is 16 (4 p.m.,) the worm displays a message in the infected systems and then shuts down Windows.

**VBS/LoveLet-BA (Visual Basic Script Worm):** This is a slight variant of VBS/LoveLet-C. The virus sends itself as an attachment to an e-mail. Infected e-mails have the subject line 'fwd: Joke' and no message body. The attachment is called 'Very funy.vbs'. Extensions targeted: vbs, vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp2, mp3. Files dropped: MSKernel32.vbs, Win32DLL.vbs, Very Funny.vbs, script.ini, Very Funny.HTM.

**WM97/Marker-ES (Word 97 Macro Virus):** This is a Word macro virus, which attempts to send user information and system details to an FTP site. On August 15th, it will also display a message box with the text "Independence Day" and "Vandhay Matharam!".

**WM97/Marker-EU (Word 97 Macro Virus):** Whenever a document on an infected system is closed, there is a 1 in 3 chance of a File Summary box appearing on the screen with the author name set to Ethan Frome.

**WM97/Melissa-BI (Word 97 Macro Virus):** This virus is a variant of WM97/Melissa. Upon initial infection, the virus sends a message to the first 50 addresses in all of the Address Books accessible by Outlook.

**W97M_Piece.A (Word 97 Macro Virus):** This is a new macro virus, which was recently reported in Europe and South America. Similar to W97M_MELISSA, this new macro virus attempts to spam copies of itself to users in the Microsoft Outlook Address book. The subject line of the outgoing message is:

"A Piece of Information From <Username>"

The body of the outgoing message is:

"Here is some thing about EME College that you better know..."

This virus also contains a destructive payload, which triggers on May 28th. On that day, it deletes all .INI files in the Windows folder, leaving the system unusable.

**WM97/Thus-AW (Word 97 Macro Virus):** This virus is a variant of the WM97/Thursday Word macro virus with no payload.

**XM97/Adn-A (Excel 97 Macro Virus):** This is a virus which contains two macros, auto_open and ClassModulo. The auto_open macro is run when the infected document is opened and instructs Excel to call the ClassModulo macro every time a new worksheet is activated. When this happens, the virus creates a file in the OFFICE directory called PERSONAL.XLA and copies the viral macros into it. This file is automatically opened every time Excel is run. From then on, it infects every workbook used.

The virus uses a random module name and on a random day changes the caption to 'SPalaci.Label.Is.Pac'. It will be loaded every time Excel is started.

**XM97/Barisada-B (Excel 97 Macro Virus):** This virus is a variant of the XM97/Barisada-A Excel macro virus. It stores its virus macros in the file RMC.XLS

On April 24, between 2pm and 3pm, the virus displays a series of dialog boxes asking the user questions which appear to be related to a fantasy role-playing game.

**XM97/Barisada-C (Excel 97 Macro Virus):** This virus is a variant of the XM97/Barisada-A Excel macro virus. It stores its virus macros in the file KHM.XLS

On April 24, between 2pm and 3pm, the virus displays a series of dialog boxes asking the user questions which appear to be related to a fantasy role-playing game.

**XM97/Laroux-NK (Excel 97 Macro Virus):** This is a virus, which contains two macros, auto_open and check_files. The auto_open macro is run when the infected document is opened, and instructs Excel to call the check_files macro every time a new worksheet is activated. When this happens, the virus creates a file in the XLSTART directory called aga.XLS and copies the viral macros into it. This file is automatically opened every time Excel is run. From then on, it infects every workbook used. The virus will be loaded every time Excel is started.

# *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last nine months, starting with CyberNotes #2000-07, and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

| Trojan | Version | Issue discussed |
|---|---|---|
| Acid Shiver + lmacid | v1.0 + 1.0Mod | CyberNotes-2000-07 |
| Asylum + Mini | v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1 | CyberNotes-2000-10,<br>CyberNotes 2000-12 |
| AttackFTP | | CyberNotes-2000-10 |
| **Backdoor/Doly.17** | | **Current Issue** |
| BF Evolution | v5.3.12 | CyberNotes-2000-10 |
| BioNet | v0.84 - 0.92 +2.2.1 | CyberNotes-2000-09,<br>CyberNotes 2000-12 |
| Bla | 1.0-5.02, v1.0-5.03 | CyberNotes 2000-09 |
| Bobo | v1.0 - 2.0 | CyberNotes-2000-09 |
| Donald Dick 2 | | CyberNotes-2000-15 |
| Drat | v1.0 - 3.0b | CyberNotes-2000-09 |
| GIP | | CyberNotes-2000-11 |
| Golden Retreiver | v1.1b | CyberNotes-2000-10 |
| ICQ PWS | | CyberNotes-2000-11 |
| ik97 | v1.2 | CyberNotes-2000-07 |
| InCommand | 1.0-1.4, 1.5 | CyberNotes-2000-09 |
| Infector | v1.0 - 1.42, v1.3 | CyberNotes-2000-07,<br>CyberNotes-2000-09 |
| iniKiller | v1.2 - 3.2, 3.2 Pro | CyberNotes-2000-09,<br>CyberNotes-2000-10 |
| Kaos | v1.1 - 1.3 | CyberNotes-2000-10 |
| Khe Sanh | v2.0 | CyberNotes-2000-10 |
| Magic Horse | | CyberNotes-2000-10 |
| Matrix | 1.4-2.0, 1.0-2.0 | CyberNotes-2000-09 |

| Trojan | Version | Issue discussed |
|---|---|---|
| **Mosaic** | **v2.00** | **Current Issue** |
| Multijoke.B | | CyberNotes-2000-15 |
| Naebi | v2.12 - 2.39, v2.40 | CyberNotes-2000-09,<br>CyberNotes 2000-12 |
| NetController | v1.08 | CyberNotes-2000-07 |
| NetSphere | v1.0 - 1.31337 | CyberNotes-2000-09 |
| Netsphere.Final | | CyberNotes-2000-15 |
| Nirvana / VisualKiller | v1.94 - 1.95 | CyberNotes-2000-07 |
| NoDesk | | CyberNotes-2000-14 |
| Omega | | CyberNotes 2000-12 |
| Phaze Zero | v1.0b + 1.1 | CyberNotes-2000-09 |
| Prayer | v1.2 - 1.5 | CyberNotes-2000-09 |
| Prosiak | beta - 0.65 – 0.70 b5 | CyberNotes-2000-09,<br>CyberNotes 2000-12 |
| **Qaz.A** | | **Current Issue** |
| Revenger | 1.0-1.5 | CyberNotes 2000-12 |
| Serbian Badman | | CyberNotes 2000-12 |
| ShitHeap | | CyberNotes-2000-09 |
| Snid | 1-2 | CyberNotes 2000-12 |
| SubSeven | V1.0-1.9b, v2.1+SubStealth, v2.2b1 | CyberNotes-2000-07 |
| Troj/Simpsons | | CyberNotes-2000-13 |
| Troj_Dilber | | CyberNotes-2000-14 |
| **TROJ_VBSWG** | | **Current Issue** |
| W32.Nuker.C | | CyberNotes-2000-14 |
| Win.Unabomber | | CyberNotes-2000-14 |
| WinCrash | Beta | CyberNotes-2000-12 |
| Winkiller | | CyberNotes 2000-12 |

**Backdoor/Doly.17:** This is a Trojan horse which is made up of two distinct parts: a client and a server. The server part of the program is installed on the infected machine, whereas the client is used by the attacking user to carry out a series of damaging actions on the computer under attack. This Trojan allows the malicious user to restart Windows, capture screenshots, close Internet connections, and remove confidential information, format the hard drive, and change mouse button functions, etc.

**Mosaic v2.00:** This is a foreign Trojan written in Visual Basic, which appears to have basic features. It infects Windows 95/98/NT. Server features include: Chat, Send keys, Execute, Open/Close CD-ROM, Ftp server, and View/Close processes.

**Qaz.A:** This is a new backdoor Trojan, which allows malicious users to access and control an infected system. It was initially distributed as "Notepad.exe" but might also appear with different filenames. Once an infected file is executed, the Trojan modifies the Windows registry so that it becomes active every time Windows is started. It also renames the original "notepad.exe" file to "note.com" and then copies itself as "notepad.exe" to the Windows folder. This way, the Trojan is also launched every time a user runs Notepad. TROJ_QAZ also attempts to spread itself to other shared drives on local networks. This Trojan does not mass e-mail itself out to lists in the user’s address book.

**TROJ_VBSWG (Aliases: VBSWG, VBS Worms Generator 1.50b):** This Trojan is a tool that generates Visual Basic Script worms. These worms can have various characters as allowed by the Trojan VBS Worm generator. This Trojan originated in Buenos Aires, Argentina. It only works if Microsoft VB5 runtimes and Windows Scripting Host 5.0 are installed or present in the infected system.